CLAIMS

What is claimed is:

1. A method for preventing writes to critical files, comprising:

(a) identifying factors associated with a computer;

(b) monitoring requests to write to files on the computer; and

(c) conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;

(d) wherein the factors are altered based on the monitoring of the requests.

2. The method as recited in claim 1, wherein the factors are selected from the group consisting of critical files, critical file locations, and trusted applications.

3. The method as recited in claim 1, wherein the factors are user configurable.

4. The method as recited in claim 1, wherein the factors are identified in a registry.

5. The method as recited in claim 2, wherein the factors include critical files associated with an operating system of the computer.

6. The method as recited in claim 2, wherein the factors include critical file locations associated with an operating system of the computer.

7. The method as recited in claim 6, wherein the critical file locations include folders.

8. The method as recited in claim 2, wherein the factors include trusted applications that initiate the requests.

9. The method as recited in claim 1, wherein the factors are updated based on a user request.

10. The method as recited in claim 1, wherein the factors are updated from a remote location via a network.

11. The method as recited in claim 1, wherein the factors are updated based on the requests.

12. The method as recited in claim 1, and further comprising conditionally preventing the writes to the files on the computer based on a user confirmation.

13. The method as recited in claim 12, wherein the factors are updated based on the user confirmation.

14. A computer program product for preventing writes to critical files, comprising:
(a) computer code for identifying factors associated with a computer;
(b) computer code for monitoring requests to write to files on the computer; and
(c) computer code for conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;
(d) wherein the factors are altered based on the monitoring of the requests.

15. The computer program product as recited in claim 14, wherein the factors are selected from the group consisting of critical files, critical file locations, and trusted applications.

16. The computer program product as recited in claim 14, wherein the factors are user configurable.

17. The computer program product as recited in claim 14, wherein the factors are identified in a registry.

18. The computer program product as recited in claim 15, wherein the factors include critical files associated with an operating system of the computer.

19. The computer program product as recited in claim 15, wherein the factors include critical file locations associated with an operating system of the computer.

20. The computer program product as recited in claim 19, wherein the critical file locations include folders.

21. The computer program product as recited in claim 15, wherein the factors include trusted applications that initiate the requests.

22. The computer program product as recited in claim 14, wherein the factors are updated based on a user request.

23. The computer program product as recited in claim 14, wherein the factors are updated from a remote location via a network.

24. The computer program product as recited in claim 14, wherein the factors are updated based on the requests.

25. The computer program product as recited in claim 14, and further comprising computer code for conditionally preventing the writes to the files on the computer based on a user confirmation.

26. The computer program product as recited in claim 25, wherein the factors are updated based on the user confirmation.

27. A system for preventing writes to critical files, comprising:
(a) logic for identifying factors associated with a computer;
(b) logic for monitoring requests to write to files on the computer; and
(c) logic for conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;
(d) wherein the factors are altered based on the monitoring of the requests.

28. A method for preventing writes to critical files, comprising:
(a) identifying an operating system associated with a computer;
(b) looking up at least one of critical files and critical file locations associated with the operating system; and
(c) preventing access to the at least one of critical files and critical file locations associated with the operating system to prevent virus proliferation.

29. A method for preventing virus proliferation, comprising:
(a) identifying an operating system;
(b) looking up critical files and critical file locations associated with the operating system;
(c) identifying additional critical files and critical file locations in a registry;
(d) identifying a plurality of trusted applications;

(e) storing the critical files, critical file locations, and trusted applications in a database;

(f) altering the database of critical files, critical file locations, and trusted applications based on a user request;

(g) updating the database of critical files, critical file locations, and trusted applications based on a remote update via a network;

(h) receiving a write request;

(i) determining whether the write request is attempting to write to one of the critical file locations in the database;

(j) if the write request is not attempting to write to one of the critical file locations in the database, permitting the write request;

(k) identifying an application that initiated the write request;

(l) determining whether the application is one of the trusted applications in the database;

(k) if the application is not one of the trusted applications in the database:

(i) alerting a user of the write request and of the application that initiated the write request,

(ii) prompting the user to confirm the write request,

(iii) if the user confirms the write request, prompting the user to confirm the write request for future write requests initiated by the application, and

(iv) if the user does confirm the write request for future write requests initiated by the application, adding the application to the database as one of the trusted applications;

(m) identifying a file associated with the write request;

(n) determining whether the write request is attempting to write to one of the critical files in the database;

(o) if the write request is attempting to write to one of the critical files in the database:

(i) alerting the user of the write request and of the critical file associated with the write request,

(ii) prompting the user to confirm the write request,

(iii) if the user confirms the write request, prompting the user to confirm the write request for future write requests associated with the critical file, and

(iv) if the user does confirm the write request for future write requests associated with the critical file, removing the critical file from the database; and

(p) if the application is one of the trusted applications in the database and if the write request is not attempting to write to one of the critical files in the database, permitting the write request.